PCT/EP00/04053

REPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

REC'D 14 JUN 2000
WIPO PCT

QL

GP 00/4053
4

09/926585

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 27 MARS 2000

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

CONFIRMATION

BREVET D'INVENTION, CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle-Livre VI

N° 55 -1328

• 26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☒

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES 01/06/99

N° D'ENREGISTREMENT NATIONAL 9907139

DÉPARTEMENT DE DÉPÔT 99

DATE DE DÉPÔT 01/06/99

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

Karine BERTHIER

THOMSON multimedia
46, quai Alphonse Le Gallo
92648 BOULOGNE CEDEX FRANCE

n°du pouvoir permanent 6075 | références du correspondant PF990030 | téléphone 01.41.86.54.88

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire ▷ demande initiale

☐ certificat d'utilité ☐ transformation d'une demande de brevet européen ▽ ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☐ non

Titre de l'invention (200 caractères maximum)

Système de tatouage de données utilisant de nouvelles méthodes d'insertion et de détection de tatouage.

3 DEMANDEUR (S) n° SIREN 3 3 3 7 7 3 1 7 4 code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination

THOMSON multimedia

Forme juridique

Société anonyme

Nationalité (s) Française

Adresse (s) complète (s) Pays

46, quai Alphonse Le Gallo
92100 BOULOGNE

FRANCE

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine	numéro	date de dépôt	nature de la demande

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(nom et qualité du signataire)

Martin KOHRS

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

RA 540 A/200298

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

CONFIRMATION

BREVET D'INVENTION, CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DEPARTEMENT DES BREVETS

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

N° D'ENREGISTREMENT NATIONAL

9907139

TITRE DE L'INVENTION :

Système de tatouage de données utilisant de nouvelles méthodes d'insertion et de détection de tatouage.

LE(S) SOUSSIGNÉ(S)

THOMSON multimedia

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique)

Teddy FURON domicilié au :

46, quai Alphonse Le Gallo
92100 BOULOGNE

et

Pierre DUHAMEL domicilié au :

46, rue Barrault
75013 PARIS

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

Boulogne, le 01.06.1999

Martin KOHRS

BA 113/140897

La présente invention se rapporte au domaine du tatouage de données numériques, appelé communément par l'expression anglaise "watermarking". Elle concerne plus particulièrement un système de tatouage de données utilisant de nouvelles méthodes d'insertion et de détection de tatouage ainsi que des dispositifs de mise en œuvre de ces méthodes.

Des méthodes récentes de protection contre la copie illicite de données numériques utilisent le principe du tatouage de données qui consiste à insérer une information de marquage, appelée communément "watermark", dans un contenu multimedia (image fixe, vidéo, son, etc.) d'une manière non perceptible. L'information de marquage, ou tatouage, peut être par exemple un signal indiquant que le contenu ne doit pas être copié ou tout autre information permettant au fournisseur du contenu multimedia de détecter les copies illégales.

Pour tenir parfaitement son rôle, le tatouage doit être robuste aux transformations du contenu tatoué, que ces transformations soient faites de manière intentionnelle par un pirate qui souhaite effacer le tatouage, ou bien qu'elles résultent de distorsions intervenues pendant la transmission du signal contenant les données tatouées.

Différentes techniques de tatouage de données sont connues de l'art antérieur. On pourra notamment se référer aux documents EP-A-0 828 372, EP-A-0 840 513, WO-A-98/03014 ou WO-A-98/54897 qui décrivent des méthodes pour insérer des tatouages dans des données à protéger et des méthodes pour détecter la présence de tels tatouages dans les données.

Un schéma généralement utilisé pour décrire le principe du tatouage de données est celui de la figure 1. Une première partie 1 concerne l'insertion d'une information cachée W (le tatouage) dans un contenu à protéger C. Il en résulte un contenu tatoué CT. La partie 2 concerne la détection de la présence de l'information W dans le contenu reçu CT. Une donnée supplémentaire K est également nécessaire dans le procédé d'insertion et de détection du tatouage. Cette donnée K qui doit être partagée de manière secrète par le dispositif d'insertion et de détection du tatouage est appelée clé par analogie aux systèmes de cryptographie dits symétriques ou à clés privées.

Par exemple, une technique connue de tatouage consiste à ajouter une séquence de pseudo bruit aléatoire à des données devant être tatouées. Le procédé de détection est fait, dans ce cas, en effectuant un calcul de

corrélation : les données reçues sont déclarées tatouées si la corrélation avec la séquence de pseudo bruit de référence (utilisée pour l'insertion du tatouage) est supérieure à un seuil donné. Dans cet exemple, la séquence de pseudo bruit de référence constitue la clé K du schéma de tatouage de données de la figure 1.

Le problème de ce schéma est que chaque entité capable de détecter le tatouage doit partager la même clé K que l'entité ayant inséré le tatouage. Dans ce cas, l'entité capable de détecter le tatouage peut en outre le supprimer ou le modifier ce qui supprime alors tout l'intérêt du tatouage initial des données. Par conséquent, un fournisseur de contenu protégé par tatouage ne doit communiquer sa clé K ayant servi à l'insertion du tatouage que de manière secrète et à des entités de confiance. Ceci limite considérablement les possibilités d'utilisation du tatouage de données dans de nombreux domaines.

En particulier, dans le domaine des appareils d'électronique grand public, il est bien connu qu'il est quasi impossible, en tout cas à des coûts raisonnables, de stocker des paramètres secrets dans un appareil ou dans un logiciel contenu dans un tel appareil. Les cartes à puces, qui sont considérées comme les seuls équipements permettant de stocker de manière sûre un paramètre secret, ne sont quant à elles pas assez puissantes pour effectuer les calculs liés à un procédé de détection de tatouage.

Dans l'exemple décrit plus haut où le tatouage est réalisé en ajoutant une séquence de pseudo bruit aléatoire aux données devant être tatouées, même si la séquence de pseudo bruit de référence est stockée de manière secrète dans le dispositif de détection du tatouage, il a été démontré qu'un pirate peut théoriquement découvrir la séquence de référence et supprimer ainsi le tatouage des données en observant la sortie du détecteur en fonction d'un grand nombre de signaux d'entrée différents.

L'invention vise à résoudre les problèmes précités.

A cet effet, l'invention concerne une méthode pour insérer une information de tatouage dans des données représentant un contenu à protéger. Selon l'invention, la méthode comprend les étapes consistant à :

a) fournir une séquence de pseudo bruit aléatoire à l'entrée d'un filtre de réponse impulsionnelle prédéfinie; et

b) ajouter ladite séquence de pseudo bruit filtrée dans lesdites données.

Selon un aspect préféré de l'invention, la méthode comprend en outre les étapes consistant à :

c) effectuer un entrelacement pseudo aléatoire des données avant l'étape b); et

d) effectuer un entrelacement inverse après l'étape b) pour obtenir les données tatouées.

L'invention concerne également une méthode pour détecter une information de tatouage dans des données représentant un contenu reçu. Selon l'invention, la méthode comprend des étapes consistant à :

i) effectuer une analyse spectrale desdites données et

ii) en déduire si lesdites données comportent une séquence de pseudo bruit qui a été filtrée par un filtre de réponse spectrale prédéfinie.

Selon un autre aspect préféré de l'invention, un entrelacement pseudo aléatoire des données reçues, identique à l'entrelacement effectué à l'étape c) ci-dessus, est effectué avant l'étape i).

L'invention concerne aussi un système de tatouage de données utilisant une méthode d'insertion de tatouage et une méthode de détection de tatouage telles que ci-dessus. Selon l'invention, une première série de paramètres, la clé privée, est utilisée pour l'insertion du tatouage et une deuxième série de paramètres, la clé publique, est utilisée pour la détection du tatouage, de telle sorte que :

- la connaissance de la clé publique ne permet pas de connaître la clé privée; et

- la connaissance de la méthode de détection et de la clé publique ne permet pas de supprimer ou de modifier le tatouage.

L'invention se rapporte également à un dispositif d'insertion d'une information de tatouage dans des données représentant un contenu à protéger. Selon l'invention, le dispositif comprend :

- des moyens de génération d'une séquence de pseudo bruit aléatoire ;

- des moyens de filtrage ayant une réponse impulsionnelle prédéfinie adaptés à recevoir ladite séquence de pseudo bruit et à fournir une séquence de pseudo bruit filtrée ; et

- des moyens d'addition de la séquence de pseudo bruit filtrée avec lesdites données.

Selon un mode de réalisation préféré se l'invention, le dispositif comporte en outre :

- des premiers moyens d'entrelacement pseudo aléatoire des données représentatives du contenu à protéger pour fournir des données entrelacées, lesdites données entrelacées étant fournies aux moyens d'addition pour être additionnées à la séquence de pseudo bruit filtrée ; et

- des moyens d'entrelacement inverse desdits premiers moyens d'entrelacement, reliés à la sortie desdits moyens d'addition pour fournir les données tatouées.

Selon un mode de réalisation particulier de l'invention, le dispositif comprend :

- des moyens de transformation du contenu à protéger en données représentatives dudit contenu ;

- des moyens de génération d'une séquence de modulation indicative de la quantité maximale de bruit pouvant être ajoutée aux dites données ;

- des premiers moyens d'entrelacement pseudo aléatoire desdites données représentatives du contenu à protéger pour fournir des données entrelacées ;

- des seconds moyens d'entrelacement pseudo aléatoire, identiques aux premiers adaptés à recevoir ladite séquence de modulation pour fournir une séquence de modulation entrelacée ;

- des moyens de multiplication adaptés à recevoir, d'une part la séquence de modulation entrelacée, et d'autre part la séquence de pseudo bruit filtrée, pour fournir l'information de tatouage ;

- des moyens d'addition des données entrelacées et de l'information de tatouage, la sortie desdits moyens d'addition étant reliée à :

- des moyens d'entrelacement inverse desdits premiers et seconds moyens d'entrelacement pour fournir les données tatouées ; et

- des moyens de transformation inverse des données tatouées en contenu marqué.

L'invention concerne également un dispositif de détection d'une information de tatouage dans des données représentant un contenu reçu. Selon l'invention, le dispositif comporte :

- des moyens d'estimation de la densité spectrale de puissance desdites données ; et

- des moyens de tests de vraisemblance d'hypothèses pour estimer si lesdites données comportent une séquence de pseudo bruit qui a été filtrée par un filtre de réponse spectrale prédéfinie.

Selon un mode de réalisation particulier, le dispositif comporte en outre :

- des moyens d'entrelacement pseudo aléatoire des données représentant le contenu reçu, adaptés à effectuer le même entrelacement que lesdits premiers moyens d'entrelacement du dispositif d'insertion, lesdites données entrelacées étant fournies aux dits moyens d'estimation de la densité spectrale de puissance.

Selon un autre mode de réalisation particulier, le dispositif comporte en outre :

- des moyens de transformation du contenu reçu en données représentatives dudit contenu, lesdits moyens de transformation étant adaptés à effectuer la même transformation que les moyens de transformation du dispositif d'insertion.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description suivante d'un mode de réalisation particulier, non limitatif, de l'invention faite en référence aux figures annexées, parmi lesquelles:

- la figure 1, décrite précédemment, illustre un schéma connu de tatouage de données numériques ;
- la figure 2 représente schématiquement un dispositif d'insertion de tatouage selon l'invention ;
- la figure 3 représente schématiquement un dispositif de détection de tatouage selon l'invention ;
- la figure 4 illustre un nouveau schéma de tatouage de données numériques selon l'invention.

Sur la figure 2, on a représenté schématiquement un dispositif selon l'invention pour insérer un tatouage dans un signal représentatif d'un contenu à protéger. Ce signal peut notamment être un signal vidéo ou audio numérique ou bien encore un signal représentant une image fixe telle qu'une photographie ou une image de synthèse calculée par ordinateur, ou plus généralement, tout signal représentant un contenu multimedia.

Tout d'abord, le contenu à protéger est transformé par un module de transformation 10 en une séquence de données numériques $\mathbf{x} = \{x_n\}$, avec n compris entre 1 et N. Par exemple, si le contenu à protéger est une image comportant N pixels, les coefficients x_n peuvent correspondre à la luminance de chaque pixel de l'image. Il peut également s'agir de coefficients de Transformée de Fourier Discrète du signal représentant le contenu à protéger, ou bien encore de coefficients de Transformée de Fourier-Mellin ou de coefficients d'une décomposition en ondelettes lorsque le contenu à protéger est une image fixe.

La séquence de données $\mathbf{x}$ représentant le contenu à protéger est transmise d'une part à un module HPM 12 fournissant en sortie une séquence de modulation $\mathbf{m} = \{m_n\}$, $\forall n \in [1..N]$. Le module HPM calcule cette séquence de modulation en fonction d'algorithmes basés sur des modèles de perception humains, tels que le modèle de l'œil de Samoff. Cette séquence $\mathbf{m} = \{m_n\}$ représente la quantité de bruit maximale qui peut être ajoutée à chaque coefficient x_n sans perte de qualité perceptible.

Selon un aspect de l'invention, la séquence de données $\mathbf{x}$ est transmise d'autre part à un entrelaceur 20, lequel effectue une permutation p aléatoire des coefficients x_n pour fournir une séquence de coefficients entrelacés $\tilde{\mathbf{x}} = \{x_{p(n)}\}$. La finalité de cet entrelacement de la séquence de données $\mathbf{x}$ sera explicitée ultérieurement.

La séquence de modulation $\mathbf{m}$ est également transmise à un entrelaceur 14 qui effectue la même permutation p des coefficients m_n que celle effectuée par l'entrelaceur 20 pour fournir en sortie une séquence de modulation entrelacée $\tilde{\mathbf{m}} = \{m_{p(n)}\}$.

Pour constituer l'information de marquage (le tatouage) qui sera insérée dans la séquence de données $\mathbf{x}$ représentant le contenu à protéger, un générateur de pseudo bruit aléatoire (non représenté) fournit tout d'abord une séquence de pseudo bruit $\mathbf{v} = \{v_n\}$, $\forall n \in [1..N]$, de distribution Gaussienne. Cette séquence de pseudo bruit $\mathbf{v}$ est transmise à l'entrée d'un filtre 16, de type Linéaire Invariant dans le Temps (LIT), dont la réponse impulsionnelle est:

$\mathbf{h} = \{h_n\}$, $\forall n \in [1..L]$ où L est un entier correspondant à la longueur du filtre;

et dont la réponse spectrale est H(f), H(f) étant la Transformée de Fourier de $\mathbf{h}$.

On obtient en sortie du filtre 16 une séquence de pseudo bruit filtrée $\mathbf{w} = \{w_n\}$, $\forall n \in [1..N]$ vérifiant l'équation (1) suivante:

$$w_n = \sum_{k=1}^{L} v_{n-k} \cdot h_k = h_n \otimes v_n \qquad \forall n \in [1..N] \tag{1}$$

dans laquelle $\otimes$ représente le produit de convolution.

On peut déduire de ceci, d'après le théorème des interférences, les deux équations suivantes (2) et (3):

$$\varphi_{ww}(\tau) = (\mathbf{h} \otimes \mathbf{h}) \otimes \varphi_{vv}(\tau) \tag{2}$$

dans laquelle $\varphi_{ww}(\tau)$ et $\varphi_{vv}(\tau)$ représentent respectivement les fonctions d'auto-corrélation de $\mathbf{w}$ et de $\mathbf{v}$; et

$$\Phi_{ww}(f) = |H(f)|^2 \cdot \Phi_{vv}(f) \tag{3}$$

dans laquelle $\Phi_{ww}(f)$ et $\Phi_{vv}(f)$ représentent respectivement les densités spectrales de puissance de $\varphi_{ww}(\tau)$ et $\varphi_{vv}(\tau)$, c'est à dire leur Transformées de Fourier.

Comme $\mathbf{v}$ est une séquence de pseudo bruit aléatoire de distribution Gaussienne, son spectre, c'est à dire la fonction $\Phi_{vv}(f)$, a une allure sensiblement plate. Par contre, une fois que cette séquence $\mathbf{v}$ est filtrée par le filtre 16, la séquence résultante $\mathbf{w}$ présente un spectre $\Phi_{ww}(f)$ qui n'est plus plat à cause du terme $|H(f)|^2$. Il est également important de noter, pour la compréhension de la suite de l'invention, que la connaissance de $|H(f)|^2$ (et par là même, la connaissance du module de $H(f)$: $|H(f)|$) ne permet pas de retrouver $H(f)$ (et donc $\mathbf{h}$) car il existe une incertitude sur la phase de $H(f)$.

En revenant à la figure 2, la séquence de pseudo bruit filtrée $\mathbf{w}$ est multipliée (multiplieur 18) par la séquence de modulation entrelacée $\tilde{\mathbf{m}}$ et la séquence résultante, qui constitue l'information de tatouage, est ajoutée (additionneur 22) à la séquence de données entrelacées $\tilde{\mathbf{x}}$.

La séquence de sortie de l'additionneur 22 est notée $\tilde{\mathbf{y}} = \{y_{p(n)}\}$ et vérifie les équations suivantes (4) et (5) :

$$y_{p(n)} = x_{p(n)} + m_{p(n)} \cdot (h_n \otimes v_n) \tag{4}$$

$$\tilde{\mathbf{y}} = \tilde{\mathbf{x}} + \tilde{\mathbf{m}} \cdot (\mathbf{h} \otimes \mathbf{v}) \tag{5}$$

La densité spectrale de puissance de la séquence de données entrelacées tatouées $\tilde{\mathbf{y}}$ est donnée par les équations suivantes (6) et (7) :

$$\Phi_{\tilde{y}\tilde{y}}(f) = \Phi_{\tilde{x}\tilde{x}}(f) + \Phi_{\tilde{m}\tilde{m}}(f) \cdot \Phi_{h \otimes v}(f) \quad (6)$$

$$\Phi_{\tilde{y}\tilde{y}}(f) = \left(\mu_x^2 \cdot \delta(f) + \sigma_x^2\right) + \left(\sigma_m^2 \cdot \sigma_v^2 \cdot \sum_u h_u^2\right) + \mu_m^2 \cdot \sigma_v^2 \cdot |H(f)|^2 \quad (7)$$

Dans l'équation (7), μ_j et σ_j représentent respectivement la moyenne et l'écart-type de la séquence $\mathbf{j} = \{j_n\}$ avec $j \in \{x, m, v\}$, $\delta(f)$ correspond à l'impulsion de Dirac et l'expression $\left(\sigma_m^2 \cdot \sigma_v^2 \cdot \sum_u h_u^2\right)$ est égale à une constante.

La séquence de données entrelacées tatouées $\tilde{\mathbf{y}}$ est ensuite transmise à un entrelaceur inverse 24 qui effectue l'opération inverse de la permutation p effectuée par les entrelaceurs 20 et 14 pour fournir une séquence de données tatouées $\mathbf{y} = \{y_n\}$ dont les coefficients se trouvent dans le même ordre que l'ordre initial des données $\mathbf{x} = \{x_n\}$.

Une transformation inverse de celle effectuée par le module de transformation 10 est ensuite effectuée par le module 26 pour obtenir le contenu marqué (ou tatoué) qui est ainsi protégé contre la copie illicite sans que le tatouage ne soit perceptible dans le contenu.

Nous allons maintenant décrire, en liaison avec la figure 3, un dispositif de détection d'un tatouage dans un contenu reçu lorsque ce tatouage a été inséré dans un contenu à protéger par un dispositif tel que celui de la figure 2.

Le principe de la détection est basée sur l'analyse spectrale du signal reçu.

Le signal reçu est représentatif du contenu reçu dont on va chercher à déterminer s'il est tatoué ou non. Ce contenu est du même type que le contenu à protéger décrit précédemment. Dans l'exemple qui va suivre, on supposera que le contenu reçu est une image contenant N pixels.

Le contenu reçu est tout d'abord transmis à un module de transformation 30 qui effectue la même opération de transformation que le module 10 du dispositif d'insertion de tatouage de la figure 2 pour fournir une séquence de données $\mathbf{r} = \{r_n\}, \forall n \in [1..N]$ représentant le contenu reçu. Dans notre exemple, on suppose que l'on obtient en sortie du module de transformation 30 les luminances r_n des pixels de l'image reçue.

Si le contenu reçu correspondait exactement au contenu tatoué issu du dispositif de la figure 2, c'est à dire si aucune transformation ou distorsion du

signal n'avait lieu pendant la transmission entre le dispositif d'insertion du tatouage et le dispositif de détection, alors on aurait :

$$\mathbb{r} = \{r_n\} = y = \{y_n\}$$

En pratique, cela n'est pas toujours le cas car le signal subit parfois des transformations pendant sa transmission.

Comme le tatouage a été inséré, dans le dispositif de la figure 2, dans une séquence de données entrelacées $\tilde{\mathbb{x}}$, on va, pour détecter la présence éventuelle d'un tatouage dans le contenu reçu, transmettre la séquence de données $\mathbb{r}$ à un entrelaceur 32 effectuant la même permutation p des coefficients r_n que celle effectuée par les entrelaceurs 20 et 14 de la figure 2.

On obtient en sortie de l'entrelaceur 32 une séquence de données entrelacées $\tilde{\mathbb{r}} = \{r_{p(n)}\}$.

On a vu précédemment que lorsque le tatouage inséré est une séquence de pseudo bruit filtrée par un filtre de réponse impulsionnelle $\mathbb{h}$ et de réponse spectrale H(f), la densité spectrale de puissance des données (entrelacées) obtenues $\tilde{y}$ est exprimée par les relations (6) et (7).

La finalité de l'entrelacement de la séquence de données $\mathbb{x}$ et de la séquence de modulation $\mathbb{m}$ va maintenant apparaître. En effet, si la séquence de données $\mathbb{x}$ représente les pixels d'une image, sa densité spectrale a une allure très structurée avec des différences d'amplitudes très importantes. Le rôle de l'entrelacement des données est de casser la cohérence statistique de cette séquence de telle sorte que la densité spectrale de la séquence de données entrelacées $\tilde{\mathbb{x}}$ ait une allure sensiblement plate, telle celle d'une séquence de pseudo bruit de distribution Gaussienne.

Ainsi, si on ajoute à cette séquence entrelacée un tatouage constitué par une séquence de pseudo bruit filtrée par un filtre de réponse spectrale H(f), on obtient une séquence de données dont la densité spectrale de puissance peut être exprimée par la relation (7) dans laquelle on peut détecter le terme significatif $|H(f)|^2$.

Le principe de la détection sera donc basé sur l'analyse spectrale de la séquence $\tilde{\mathbb{r}}$ et sur un test de vraisemblance d'hypothèses, l'hypothèse testée étant la suivante : si la séquence de données entrelacées $\tilde{\mathbb{r}}$ contient du bruit, est-ce un bruit qui a été filtré par un filtre dont la réponse spectrale a un module similaire à |H(f)| ? Si la réponse est oui, on en déduira que le bruit

présent dans la séquence $\tilde{r}$ est un tatouage et, dans le cas contraire, on en conclura que le contenu reçu n'était pas tatoué.

En pratique, cette analyse est basée sur des calculs d'analyse spectrale et de test de vraisemblance d'hypothèses qui sont décrits de manière détaillée dans l'ouvrage de K. Dzhaparidze, "*Parameter Estimation and Hypothesis Testing in Spectral Analysis of Stationary Time Series*", Springer Series in Statistics, Springer-Verlag, 1986, auquel on pourra se référer pour plus de détails.

En revenant à la figure 3, la séquence de données reçues entrelacées $\tilde{r}$ est transmise à un module 34 effectuant un calcul de Periodogramme. Ce calcul vise à estimer la densité spectrale de puissance de la séquence $\tilde{r}$. On obtient en sortie une grandeur $I_N(f)$ donnée par la relation (8) suivante :

$$I_N(f) = \frac{1}{N}\left|\sum_{k=1}^{N} \tilde{r}_k \cdot \exp(2\pi j f k)\right|^2 \qquad (8)$$

Cette grandeur est ensuite transmise à un module 36 effectuant un test de vraisemblance d'hypothèses pour déterminer si le contenu reçu est tatoué (réponse en sortie "O") ou non (réponse en sortie "N").

Le module 36 teste la vraisemblance de deux hypothèses :

- selon la première hypothèse G_0, le contenu reçu n'est pas tatoué, donc la densité spectrale de la séquence $\tilde{r}$ est sensiblement plate et peut être estimée par la relation (9) suivante :

$$g_0(f) = \sigma_r^2 + \mu_r^2 \cdot \delta(f) \qquad (9)$$

- selon la deuxième hypothèse G_1, le contenu reçu est tatoué et la densité spectrale de la séquence $\tilde{r}$ peut être estimée par la relation (10) suivante :

$$g_1(f) = \mu_m^2 \cdot \sigma_v^2 \cdot |H(f)|^2 + C \qquad (10)$$

dans laquelle C est une constante et σ_v est égal à 1 (on choisit préférentiellement la séquence de pseudo bruit v au niveau du dispositif d'insertion de telle sorte que σ_v soit égal à 1, mais on peut également choisir d'autres valeurs). En outre, μ_m est nommée au niveau du dispositif d'insertion et vaut par exemple 3.

Pour estimer la vraisemblance des hypothèses G_0 et G_1, le module 36 calcule deux nombres $U_{N,0}(\tilde{r})$ et $U_{N,1}(\tilde{r})$ représentant les vraisemblances des hypothèses G_0 et G_1 selon la relation (11) suivante :

$$U_{N,i}(\tilde{r}) = -\int_{-\frac{1}{2}}^{\frac{1}{2}} \left(\log g_i(f) + \frac{I_N(f)}{g_i(f)} \right) df \qquad \text{avec } i \in \{0, 1\} \qquad (11)$$

En effectuant ensuite une comparaison de ces deux nombres, le module 36 en déduit :

- si $U_{N,1}(\tilde{r}) > U_{N,0}(\tilde{r})$, alors la réponse du détecteur est "O" signifiant que le contenu reçu est tatoué ; et
- si $U_{N,1}(\tilde{r}) < U_{N,0}(\tilde{r})$ alors la réponse du détecteur est "N" signifiant que le contenu reçu n'est pas tatoué.

On peut également, de manière préférentielle, calculer la différence $(U_{N,1}(\tilde{r}) - U_{N,0}(\tilde{r}))$ et n'effectuer les comparaison ci-dessus que si cette différence est supérieure à un seuil prédéterminé, ceci afin de garantir une meilleure exactitude de la détection.

Les méthodes d'insertion et de détection de tatouage qui viennent d'être décrites en référence aux figures 2 et 3 permettent de réaliser un nouveau système de tatouage qui est illustré par la figure 4. Dans ce nouveau système et selon un aspect préféré de l'invention, on utilise pour l'insertion (100) d'un tatouage W dans un contenu C, un paramètre que l'on appelle "clé privée" K_{PRI}, tandis que pour la détection (200) d'un tatouage dans un contenu reçu CT, on utilise un autre paramètre que l'on appelle "clé publique" K_{PUB}. Les termes "clé privée" et "clé publique" sont utilisés par analogie aux systèmes cryptographiques à clés publiques. On notera que le tatouage W est ici binaire, c'est à dire que, soit le contenu C est tatoué, soit il ne l'est pas, mais W ne contient pas d'information propre.

Dans le mode de réalisation qui a été décrit plus haut, la clé privée K_{PRI} est formée par la séquence de pseudo bruit aléatoire $\mathbf{v}$ ainsi que par la réponse impulsionnelle $\mathbf{h}$ du filtre 16 (Fig. 2). Les séquences $\mathbf{v} = \{v_n\}$ et $\mathbf{h} = \{h_n\}$ sont en effet indispensables au calcul de la séquence $\mathbf{w} = \{w_n\}$ qui elle-même, après avoir été multipliée par la séquence de modulation entrelacée $\tilde{\mathbf{m}}$ est insérée dans les données représentant le contenu à protéger.

La clé publique utilisée pour détecter le tatouage dans le contenu reçu est quant à elle formée du module de la réponse spectrale du filtre 16 $|H(f)|$. En effet, dans les calculs d'analyse spectrale effectués (modules 34 et 36 de la figure 3) pour détecter la présence d'un tatouage dans un contenu reçu CT, seule la connaissance de $|H(f)|$ est nécessaire. En particulier, il n'est pas

nécessaire de connaître $\mathbf{v}$ et $\mathbf{h}$ (la clé privée) pour effectuer la détection du tatouage. Or, comme on l'a vu plus haut dans la description, la connaissance de $|H(f)|$ ne suffit pas pour connaître $H(f)$ et donc $\mathbf{h}$.

On obtient donc un système dans lequel la connaissance de la clé publique ne permet pas d'en déduire la clé privée. Et ne connaissant pas la clé privée, il est impossible pour le dispositif effectuant la détection du tatouage de le supprimer ou de le modifier. La détection peut donc être effectuée dans un environnement non sécurisé sans risque que le tatouage soit effacé.

REVENDICATIONS

1. Méthode pour insérer une information de tatouage dans des données (**x**) représentant un contenu à protéger, caractérisée en ce qu'elle comprend les étapes consistant à :

a) fournir une séquence (**v**) de pseudo bruit aléatoire à l'entrée d'un filtre de réponse impulsionnelle prédéfinie (**h**) ; et

b) ajouter ladite séquence de pseudo bruit filtrée (**w**) dans lesdites données.

2. Méthode selon la revendication 1, caractérisée en ce qu'elle comprend en outre les étapes consistant à :

c) effectuer un entrelacement (p) pseudo aléatoire des données (**x**) avant l'étape b) ; et

d) effectuer un entrelacement inverse après l'étape b) pour obtenir les données tatouées.

3. Méthode pour détecter une information de tatouage dans des données (**r**) représentant un contenu reçu, caractérisée en ce qu'elle comprend des étapes consistant à :

i) effectuer une analyse spectrale desdites données ; et

ii) en déduire si lesdites données comportent une séquence de pseudo bruit qui a été filtrée par un filtre de réponse spectrale (H(f)) prédéfinie.

4. Méthode selon la revendication 3 pour détecter une information de tatouage dans des données (**r**) représentant un contenu reçu, l'information de tatouage étant adaptée à être insérée suivant la méthode selon la revendication 2, caractérisée en ce qu'elle comprend en outre une étape consistant à :

iii) effectuer, avant l'étape i), un entrelacement pseudo aléatoire (p) des données (**r**) reçues, identique à l'entrelacement effectué à l'étape c).

5. Système de tatouage de données utilisant une méthode d'insertion de tatouage selon l'une des revendications 1 ou 2 et une méthode de détection de tatouage selon l'une des revendications 3 ou 4, caractérisé en

ce qu'une première série de paramètres (**v**, **h**), la clé privée (K_{PRI}), est utilisée pour l'insertion du tatouage et une deuxième série de paramètres (|H(f)|), la clé publique (K_{PUB}), est utilisée pour la détection du tatouage, de telle sorte que :

- la connaissance de la clé publique ne permet pas de connaître la clé privée ; et
- la connaissance de la méthode de détection et de la clé publique ne permet pas de supprimer ou de modifier le tatouage.

6. Dispositif d'insertion d'une information de tatouage dans des données (**x**) représentant un contenu à protéger, caractérisé en ce qu'il comprend :

- des moyens de génération d'une séquence de pseudo bruit aléatoire (**v**) ;
- des moyens de filtrage (16) ayant une réponse impulsionnelle (**h**) prédéfinie adaptés à recevoir ladite séquence de pseudo bruit (**v**) et à fournir une séquence de pseudo bruit filtrée (**w**) ; et
- des moyens d'addition (22) de la séquence de pseudo bruit filtrée (**w**) avec lesdites données (**x**).

7. Dispositif selon la revendication 6, caractérisé en ce qu'il comporte en outre :

- des premiers moyens (20) d'entrelacement pseudo aléatoire des données (**x**) représentatives du contenu à protéger pour fournir des données entrelacées ($\tilde{\mathbf{x}}$), lesdites données entrelacées étant fournies aux moyens d'addition (22) pour être additionnées à la séquence de pseudo bruit filtrée (**w**) ; et
- des moyens (24) d'entrelacement inverse desdits premiers (20) moyens d'entrelacement, reliés à la sortie desdits moyens d'addition (22) pour fournir les données tatouées.

8. Dispositif selon la revendication 6, comprenant :

- des moyens (10) de transformation du contenu à protéger en données (**x**) représentatives dudit contenu ;
- des moyens (12) de génération d'une séquence de modulation (**m**) indicative de la quantité maximale de bruit pouvant être ajoutée auxdites données ;

caractérisé en ce qu'il comprend en outre :

- des premiers moyens (20) d'entrelacement pseudo aléatoire desdites données (x) représentatives du contenu à protéger pour fournir des données entrelacées ($\tilde{x}$) ;

- des seconds moyens (14) d'entrelacement pseudo aléatoire, identiques aux premiers (20) adaptés à recevoir ladite séquence de modulation (m) pour fournir une séquence de modulation entrelacée ($\tilde{m}$) ;

- des moyens de multiplication (18) adaptés à recevoir, d'une part la séquence de modulation entrelacée ($\tilde{m}$), et d'autre part la séquence de pseudo bruit filtrée (w), pour fournir l'information de tatouage ;

- des moyens (22) d'addition des données entrelacées ($\tilde{x}$) et de l'information de tatouage, la sortie desdits moyens d'addition étant reliée à :

- des moyens (24) d'entrelacement inverse desdits premiers (20) et seconds (14) moyens d'entrelacement pour fournir les données tatouées (y) ; et

- des moyens (26) de transformation inverse des données tatouées en contenu marqué.

9. Dispositif de détection d'une information de tatouage dans des données (r) représentant un contenu reçu, caractérisé en ce qu'il comporte :

- des moyens (34) d'estimation de la densité spectrale de puissance desdites données ; et

- des moyens (36) de tests de vraisemblance d'hypothèses pour estimer si lesdites données comportent une séquence de pseudo bruit qui a été filtrée par un filtre de réponse spectrale (H(f)) prédéfinie.

10. Dispositif selon la revendication 9, adapté à détecter une information de tatouage insérée par un dispositif d'insertion selon l'une des revendications 7 ou 8, caractérisé en ce qu'il comporte :

- des moyens (32) d'entrelacement pseudo aléatoire des données (r) représentant le contenu reçu, adaptés à effectuer le même entrelacement (p) que lesdits premiers moyens d'entrelacement (20) du dispositif d'insertion, lesdites données entrelacées ($\tilde{r}$) étant fournies aux dits moyens (34) d'estimation de la densité spectrale de puissance.

11. Dispositif selon la revendication 10, adapté à détecter une information de tatouage insérée par un dispositif d'insertion selon la revendication 8, caractérisé en ce qu'il comporte en outre :

- des moyens de transformation (30) du contenu reçu en données (r) représentatives dudit contenu, lesdits moyens de transformation étant adaptés à effectuer la même transformation que les moyens de transformation (10) du dispositif d'insertion.

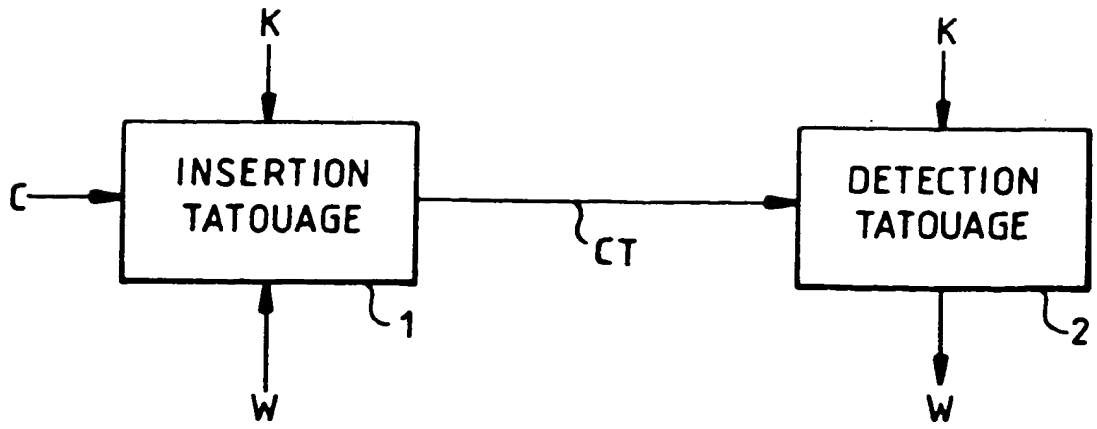
K
K
C
INSERTION TATOUAGE
DETECTION TATOUAGE
CT
1
2
W
W

FIG.1

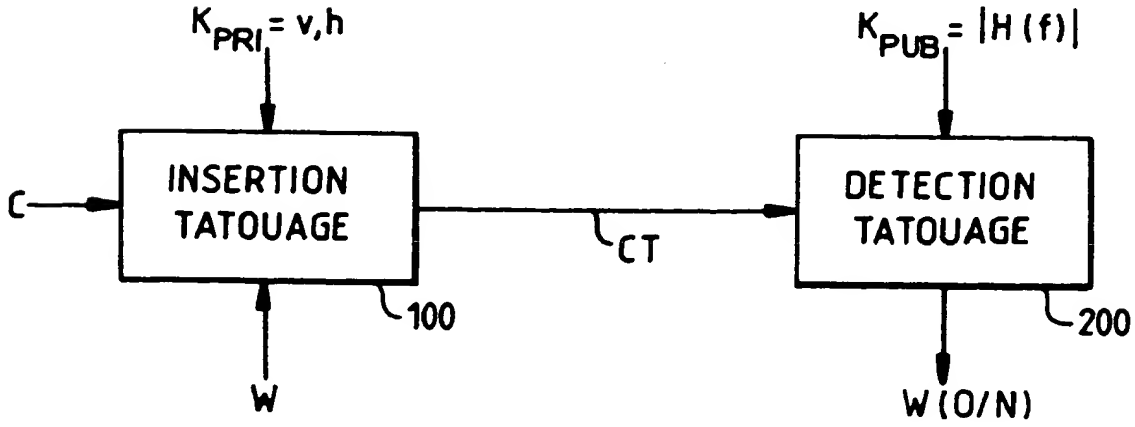
K_{PRI} = v,h
K_{PUB} = |H(f)|
C
INSERTION TATOUAGE
DETECTION TATOUAGE
CT
100
200
W
W(O/N)

FIG.4

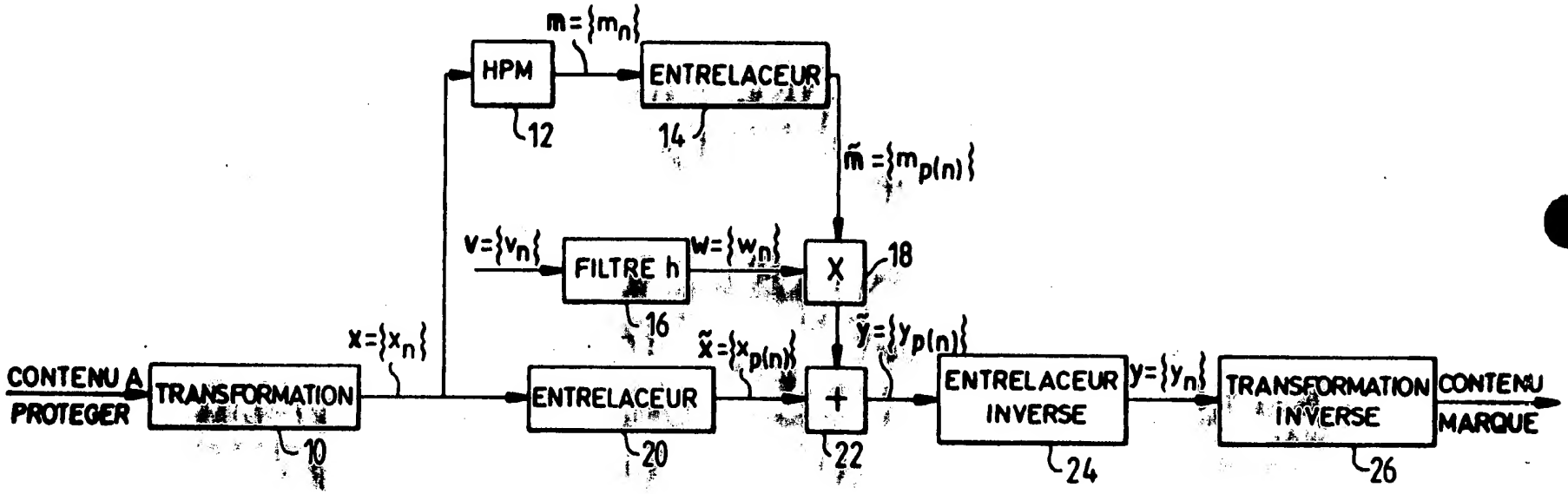
m={m_n}
HPM
ENTRELACEUR
12
14
m̃={m_p(n)}
v={v_n}
FILTRE h
w={w_n}
X
18
16
x={x_n}
x̃={x_p(n)}
ỹ={y_p(n)}
CONTENU A PROTEGER
TRANSFORMATION
ENTRELACEUR
+
ENTRELACEUR INVERSE
y={y_n}
TRANSFORMATION INVERSE
CONTENU MARQUE
10
20
22
24
26

FIG. 2

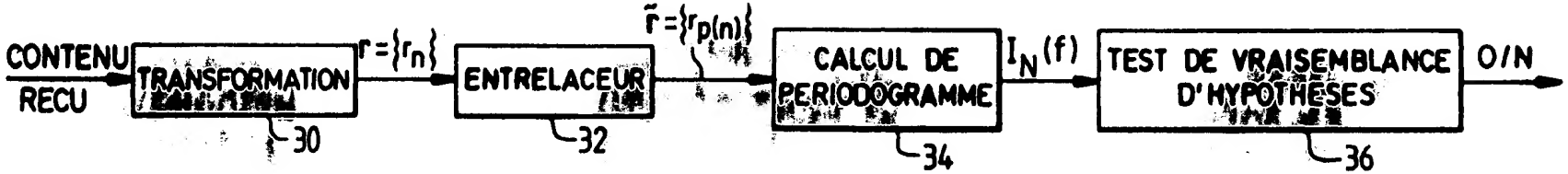
CONTENU RECU
TRANSFORMATION
r={r_n}
ENTRELACEUR
r̃={r_p(n)}
CALCUL DE PERIODOGRAMME
I_N(f)
TEST DE VRAISEMBLANCE D'HYPOTHESES
O/N
30
32
34
36

FIG. 3